UNIVERSITAT JAUME I

Trabajo Fin de Grado

Hacia un nuevo paradigma en la protección de datos

Presentado por:

Silvia Grangel Tomás

Tutor/a:

Félix Francisco Serrano Gallardo

Grado en Derecho

Curso académico 2017/18

ÍNDICE

I. Abreviaturas

AEPD	Agencia Española de Protección de Datos
Art.	Artículo
CE	Constitución española
CEDH	Convenio Europeo de Derechos Humanos
CP	Código Penal
DNI	Documento Nacional de Identidad
DPO	Delegado de Protección de Datos
LOPD	Ley Orgánica de Protección de Datos
LPJSP	Ley del Régimen Jurídica del Sector Público
RGPD	Reglamento General de Protección de Datos
STC	Sentencia del Tribunal Constitucional
TFUE	Tratado de Funcionamiento de la Unión Europea
UE	Unión Europea

I. Introducción

La Constitución Española en su artículo 18.4 se hacía eco de los trabajos desarrollados a finales de 1960 en el Consejo de Europa con el reconocimiento de la protección de las personas físicas en relación con el tratamiento de datos personales.

El aumento de los flujos transfronterizos de datos personales como consecuencia del mercado interior, junto con la vertiginosa evolución tecnológica y la globalización, han dado como consecuencia que los datos personales sean el recurso fundamental de la sociedad de la información. Debido a ello, se han intensificado los medios tendentes a garantizar la protección de los datos personales, y lograr la uniformidad legislativa en Europa en la materia.

Las estadísticas sobre sociedad y economía digital realizadas por Eurostat demuestran que en 2007 se superó un hito cuando la mayoría de los hogares de Europa, un 55%, contaban con acceso a Internet. Esta proporción no ha hecho más que aumentar hasta que en 2016 se alcanzó el 85% como consecuencia de que las TIC se han convertido en un bien a disposición del público en general por su accesibilidad y coste.

Las encuestas sobre privacidad y protección de la identidad personal demuestran que en 2016 en los Estados miembros de la UE más de un 70% de los usuarios de Internet facilitaron algún tipo de dato personal por esta vía. Muchos de ellos llegaron a emprender acciones para controlar el acceso a sus datos personales en Internet. Casi la mitad (el 46%) de todos los usuarios de Internet se negaron a permitir el uso de datos personales con fines publicitarios y dos quintos (un 40%) limitaron el acceso a su contenido en las redes sociales.

Hay que destacar que más de un tercio (37%) de los usuarios de Internet leyó las políticas de privacidad antes de facilitar sus datos personales, mientras casi un tercio (31%) restringió el acceso a su localización geográfica.[1]

En 2016, el 71% de las personas comprendidas entre los 16 y los 74 años de edad que habían usado Internet en los doce meses anteriores sabían que se podían usar cookies para hacer un seguimiento de la persona en Internet. El conocimiento sobre esta cuestión era ligeramente más elevado entre los usuarios de menor de edad.

En España han tenido una gran repercusión las novedades introducidas en materia de protección de datos personales por el Reglamento General de Protección de Datos, mostrándose en las estadísticas mensuales del Registro General de Protección de Datos, más concretamente en la de marzo de 2018. En la estadística mensual sobre el resumen de operaciones de inscripción a instancias del interesado evidencia un gran número de altas: 43.785. También hubo un total de 7.306 modificaciones y 4.479 supresiones. Por lo que el total de operaciones fue realmente alto, que sumado al resto de los meses de 2018 comporta ya un total de 166.883 operaciones.[2]

El presente trabajo tiene como objetivo realizar un recorrido analítico desde la primera vez que el legislador reconoció el derecho a la protección de la privacidad en la legislación, y su evolución hasta llegar a la actual regulación europea y nacional. Más específicamente, desde que se reconoció el derecho a la protección de datos en 1950 por el Convenio Europeo de Derechos Humanos, hasta llegar al Reglamento General de Protección de Datos, en vigor en toda la UE desde el 25 de mayo pasado, y el actual Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal en tramitación parlamentaria en el Congreso de los Diputados español.

[1] http://ec.europa.eu/eurostat/ Datos de Eurostat [fecha de consulta: 01/05/2018]

[2] http://www.agpd.es/

Además, se estudiarán las novedades más relevantes que introduce la nueva normativa como la figura jurídica del llamado Delegado de Protección de Datos (Data Protection Officer), qué se entiende por dato personal y cómo se regula, así como el tratamiento del consentimiento, las categorías especiales de datos personales, y el régimen sancionador en la protección de datos.

Por su complejidad y extensión, no se ha podido profundizar en las demás novedades que se incorporan a nuestro ordenamiento jurídico por el Reglamento. Se citarán, no obstante, nuevos derechos del ciudadano como el derecho al olvido, el nuevo derecho a la portabilidad, la incorporación del principio de responsabilidad proactiva, la obligación de notificar las violaciones de seguridad, y la regulación de transferencias internacionales de datos.

En el primer capítulo se aborda la evolución del derecho a la protección de datos, y el esfuerzo llevado a cabo por las instituciones europeas con el objetivo de darle la mayor protección posible y la armonización de la legislación de los Estados miembros en la materia para favorecer el mercado interior. Fruto de este esfuerzo es el Reglamento General de Protección de Datos, directamente aplicable desde mayo de 2018. Se tratan también brevemente las principales novedades. A colación de ello, se habla de la protección de datos de carácter personal en nuestro país.

En el segundo capítulo se analiza la protección de datos personales. Primero se habla de la evolución que ha tenido el derecho fundamental a la protección de datos personales y de las principales sentencias de nuestro país al respecto, para en segundo lugar definir qué se entiende por dato personal.

También se estudia el tratamiento del consentimiento introducido por el Reglamento, su licitud y condiciones, así como la nueva regulación para el consentimiento del menor. Para finalizar este capítulo se tratan las categorías especiales de datos personales, entre las que se encuentran dos categorías reguladas por primera vez: los datos genéticos y datos biomédicos.

En el tercer capítulo se estudia la figura del Delegado de Protección de Datos, introducida por el Reglamento, que aunque en algunos países como Alemania o Francia ya existía, supone una novedad para nuestro país. Con el Delegado se pretende fomentar el derecho fundamental a la protección de datos. Se define qué es un Delegado de Protección de Datos y las características que ha de poseer. También se analizan como deberán ser designados y las funciones que habrán de realizar. Además, se realiza una comparación con otras figuras afines como son el Compliance Officer, el Responsable del fichero o del tratamiento, y el Encargado del tratamiento. Todas figuras similares pero que realizan funciones diferentes de manera que se pueda dar una cobertura total a la protección de datos.

Finalmente, se analizan también las responsabilidades en que se puede incurrir, ya que el Reglamento ha regulado un amplio marco de deberes que se deben respetar en el desarrollo de datos personales. En este apartado se hablará de la responsabilidad penal contemplada en el artículo 197 del Código Penal español, de la responsabilidad administrativa, y para concluir, de la responsabilidad civil.

Desde el 25 de mayo de 2018 el Reglamento General de Protección de Datos es directamente aplicable en los países miembros. Pretende adaptar la legislación a la actualidad y dar una cobertura en protección digital sin precedentes. Comporta una nueva etapa en Europa reflejo de la rápida evolución tecnológica. Debido a ello, y por el interés que suscita la creación de la nueva figura jurídica del Delegado de Protección de Datos como posibilidad futura de trabajo para juristas, el nuevo RGPD fue el tema escogido para la realización de este estudio.

II. LA PROTECCIÓN DE LA PRIVACIDAD

1. Normativa Europea sobre la protección de la privacidad:

1.1. Antecedentes en la Unión Europea: desde los inicios de la protección de la privacidad al actual sistema.

El análisis de los antecedentes normativos de protección de datos en Europa debe comenzar hablando de los instrumentos utilizados por el Consejo de Europa: el Convenio Europeo de Derechos Humanos de 1950 (CEDH), y el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981 (Convenio 108).

El CEDH, ratificado por España en 1979, en su artículo 8.1, reconoce el derecho a la protección de datos, apartado esencial que fue el punto de partida de toda la regulación europea posterior sobre la protección de datos, y que establece los requisitos para poder justificar una posible injerencia por la autoridad pública en este derecho.

Se debe resaltar la gran importancia que ha tenido como antecedente el Convenio 108 ya que fue el primer instrumento jurídico vinculante en protección de datos personales.

Establecidas las bases de la protección de la privacidad en la legislación de la Unión Europea, los Estados miembros regularon mediante instrumentos propios el derecho a la protección de datos. Esto dio lugar a que no hubiera uniformidad en la materia, por lo que se obstaculizaba la realización del mercado interior de la UE.

Debido a ello se decidió adoptar "un instrumento jurídico propio de la Unión Europea en materia de protección de datos que garantizara un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la

vida privada de las personas y facilitar el desarrollo del mercado interior dentro de la Unión Europea".[3]

Se adoptó la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que fue el primer hito en la regulación de la protección de datos en la UE. La misma fue la base para la regulación actual del Reglamento General de Protección de datos, aplicable desde el 25 de mayo de 2018.

La Directiva 95/46/CE entró en vigor en 1995 y tuvo como objetivos principales armonizar los instrumentos nacionales de protección de datos mediante la aproximación de legislaciones para asegurar el funcionamiento del mercado interior, eliminar los obstáculos a la libre circulación de datos personales, y mantener un nivel de protección de los derechos y libertades de las personas que fuera equivalente en todos los Estados miembros. [4]

La Comisión Europea realizó informes sobre la aplicación de la Directiva mientras estuvo vigente, mostrando su eficiencia en la protección de datos y su utilidad práctica para la sociedad. Sin embargo, la rápida evolución social llevó a que la Directiva 95/46/CE dejase de dar una respuesta a las necesidades sociales en protección de la privacidad. Por ello, en 2010 la Comisión Europea asumió que había nuevos retos, y nuevos problemas a los que dar respuesta.

Un factor que afectó de manera decisiva el impulso de una nueva regulación fue la entrada en vigor en 2009 del Tratado de Lisboa, ya que reconoció a la Carta de Derechos Fundamentales de la Unión Europea como jurídicamente vinculante.
Y como consecuencia, el derecho a la protección de datos personas se elevó a

[3] FERNÁNDEZ CONTE, Julen y LEÓN BURGOS, Diego, <<Antecedentes y proceso de reforma sobre protección de datos en la Unión Europea>>, en María Álvarez Caro y Miguel Recio Gayo (coord.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*, Editorial Reus, Madrid, 2016, pp. 35-50, en p.37

[4] FERNÁNDEZ CONTE, Julen y LEÓN BURGOS, Diego, <<Antecedentes y proceso de reforma sobre protección..>>, cit., p. 38.

la categoría de derecho fundamental. Además, se introdujo una disposición específica en el Tratado de Funcionamiento de la Unión Europea que codificaba el derecho de toda persona a la protección de datos personales.

La Comisión decidió que el mejor instrumento jurídico para llevar a cabo la modificación era un Reglamento en base al artículo 288 TFUE que establece su alcance general, la obligatoriedad en todos sus elementos y por ser directamente aplicable en cada Estado miembro sin requerir trámites especiales para ello. Así se conseguiría reducir la fragmentación jurídica de los Estados miembros y ofrecer una mayor seguridad jurídica.

La propuesta de Reglamento se basó en el artículo 16 del TFUE, disposición que permite la adopción de normas relativas a la protección de las personas físicas con respecto al tratamiento de datos de carácter personal por parte de los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión.[5]

El 25 de enero de 2012 la Comisión Europea presentó la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, también denominado Reglamento General de Protección de Datos (RGPD). La Propuesta incluiría los principios de transparencia y de responsabilidad de los controladores por su procesamiento. Estableció criterios para el procesamiento adecuado de los datos personales, así como el consentimiento previo al uso y el derecho a ser informados sobre el período de conservación de los mismos, y el "derecho a ser olvidado".

En el proceso de creación del nuevo Reglamento, los Estados miembros analizaron con detalle aspectos la sentencia que se había dictado en el asunto Google contra España que trataba el derecho al olvido y como equilibrarlo con el derecho a la libertad de expresión, ambos de gran importancia hoy en día y

[5] FERNÁNDEZ CONTE, Julen y LEÓN BURGOS, Diego, <<Antecedentes y proceso de reforma sobre protección..>> cit., p. 43.

estrechamente relacionados.[6] La citada sentencia es la Sentencia del Tribunal de Justicia de 13 de mayo de 2014: litigio entre Google Spain, y Google Inc., por un lado, y la Agencia Española de Protección de Datos («AEPD») y el Sr. Costeja González, por otro, en relación con una resolución de dicha Agencia por la que se estimó la reclamación del Sr. Costeja González contra ambas sociedades y se ordenaba a Google Inc. que adoptara las medidas necesarias para retirar los datos personales del Sr. Costeja González de su índice e imposibilitara el acceso futuro a los mismos.

Esta reclamación se basaba en que, cuando un internauta introducía el nombre del Sr. Costeja González en el motor de búsqueda de Google, obtenía como resultado vínculos hacia dos páginas del periódico “La Vanguardia” en las que figuraba un anuncio de una subasta de inmuebles relacionada con un embargo por deudas a la Seguridad Social, que le mencionaba. El reclamante solicitaba, que se exigiese a “La Vanguardia” eliminar o modificar la publicación para que no apareciesen sus datos personales, o utilizar las herramientas facilitadas por los motores de búsqueda para proteger estos datos. Y también que se exigiese a Google Spain o a Google Inc. que eliminaran u ocultaran sus datos personales para que dejaran de incluirse en sus resultados de búsqueda y dejaran de estar ligados a los enlaces de “La Vanguardia”. En este marco, el Sr. Costeja González afirmaba que el embargo al que se vio sometido en su día estaba totalmente solucionado y resuelto desde hace años y carecía de relevancia actualmente.

El Tribunal declaró que, para respetar los derechos que se establecían en las disposiciones de la Directiva 95/46, el gestor de un motor de búsqueda estaba obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contuviesen información relativa a esta persona; también en el supuesto de que este nombre o esta información no se borrasen previa o simultáneamente de estas páginas web, y, en su caso, aunque la

[6] https://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_justicia/common/3._Sentencia_Gran_Sala_de_13_de_mayo_de_2014...[consulta: 20/03/2018]

publicación en dichas páginas sea en sí misma lícita. Añadía que el interesado tiene derecho a que, en la situación actual, la información en cuestión relativa a su persona ya no esté vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado. [7]

El interesado puede, habida cuenta de los derechos que le reconocen los artículos 7 y 8 de la Carta, solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate.

Cabe resaltar el acuerdo al que se llegó en marzo de 2015 en el proceso de tramitación del nuevo Reglamento por las instituciones europeas. En él se adoptó un enfoque parcial en materia de principios generales, que son los que dieron forma al Reglamento.[8] El Parlamento y el Consejo lograron alcanzar el acuerdo, que se ratificó oficialmente por el Consejo en febrero de 2016. De este modo, el 27 de abril de 2016 el DOUE publicó el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se derogaba la Directiva 95/46/CE.

---

7 https://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_justicia/common/3._Sentencia_Gran_Sala_de_13_de_mayo_de_2014...[consulta: 20/03/2018]

8 FERNÁNDEZ CONTE, Julen y LEÓN BURGOS, Diego, <<Antecedentes y proceso de reforma sobre protección..>>, cit., p. 48.

En la UE la protección de datos de carácter personal se ha convertido en un derecho fundamental de toda persona, protegido por el Reglamento General de Protección de Datos, con el objetivo de "fortalecer, homogeneizar y consolidar el nivel de protección de los derechos de las personas y titulares de datos en toda la Unión Europea"[9]

1.2. El Reglamento General de Protección de Datos:

a) Principales novedades:

El objeto del Reglamento es doble, y viene establecido en su artículo 1.1: *"el presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos"*.

El Reglamento introduce una serie de novedades:[10]

- La definitiva consolidación de la protección de datos como derecho fundamental, la extensión del ámbito territorial de aplicación de las normas protectoras de la privacidad (art. 3). En el RGPD se trata la protección de datos como un derecho fundamental no absoluto, sino que debe entenderse en relación con su función en la sociedad y mantener el equilibro con otros derechos fundamentales, atendiendo al principio de proporcionalidad.
- La definición y regulación del consentimiento (arts. 4.11 y 7). Se debe destacar la determinación de la edad en la que los menores pueden consentir el tratamiento de sus datos en Internet. Se considerará lícito cuando tenga como mínimo 16 años. Si es menor de 16 años el tratamiento sólo se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño.

  Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

[9] FERNÁNDEZ CONTE, Julen y LEÓN BURGOS, Diego, <<Antecedentes y…>>, cit., p. 50

[10] Dossier: Manual de las principales novedades del Reglamento Europeo de Protección de Datos, Editorial Thomson Reuters, 1 de marzo de 2018.

También se impone que el consentimiento para tratar datos personales, sea libre, informado, específico e inequívoco. El consentimiento debe prestarse mediante una acción positiva del interesado, y para los datos sensibles, como origen étnico, opiniones políticas, salud y orientación sexual, se requiere un consentimiento explícito.

Además el consentimiento obtenido debe ser verificable.

- La regulación del derecho al olvido en el art. 17, que establece: "*El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan*", cuando concurran las circunstancias determinadas por el mismo.
- La regulación del nuevo derecho a la portabilidad en el art. 20, lo cual supone que el interesado: *"Tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado".*
- La incorporación del principio de responsabilidad proactiva (*accountability*) en el artículo 24 impone al responsable y al encargado del tratamiento estar en condiciones de demostrar que cumplen con las previsiones normativas en materia de protección de datos de carácter personal.

  Además en el art 32 se determinan una serie de medidas que deberán ser implementadas, como el cifrado de datos personales.
- La exigencia de tener en cuenta los principios de privacidad desde el diseño y por defecto (art. 25). Y para llevar a cabo este objetivo el artículo 25 dispone: *"el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas.* [11]
- La no necesidad de inscribir los ficheros, aunque sea necesario que los responsables y encargados lleven un registro de las actividades del tratamiento, que estará a disposición de las autoridades de control (art. 30).

[11] Dossier: Manual de las principales novedades del Reglamento..., cit.

- La obligación de notificar las violaciones de seguridad, tanto a las Autoridades de Protección de Datos como incluso a los propios afectados que se recogen en los artículos 33 y 34 del RGPD. El responsable del tratamiento debe documentar cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas.
- La regulación de la evaluación de impacto relativa a la protección de datos (art 35).
- La consulta previa al tratamiento si éste entraña un alto riesgo (art. 36).
- El impulso a la creación de mecanismos de certificación y sellos y marcas de protección de datos (art. 42-43).
- La regulación de las transferencias internacionales con una referencia expresa a las normas corporativas vinculantes como legitimadoras de las transferencias (art. 47).
- El régimen de las autoridades independientes de control (arts. 51 a 56) y el mecanismo de cooperación y coherencia (arts. 60 a 67).
- La nueva regulación del Comité Europeo de Protección de Datos (arts. 68 a 76).
- El régimen de recursos, responsabilidad y sanciones (arts. 77 a 84). En particular el que toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos; y que el importe de las multas puede ahora llegar hasta 20.000.000 de euros, o si se trata de empresas, hasta un 4% del volumen del negocio total anual global.[12]

El objeto y el ámbito de aplicación del RGPD son los mismos que se recogía en la Directiva 95/46/CE. Se excluye del ámbito de aplicación los tratamientos de datos policiales y judiciales, sobre lo que la anterior Directiva no se pronunciaba.

[12] PIÑAR MAÑAS, José Luis.; <<Introducción. Hacia un nuevo modelo europeo de protección de datos>> en María Álvarez Caro y Miguel Recio Gayo (coord.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*, Editorial Reus, Madrid, 2016, pp.15-22, p.19.

El Reglamento es de aplicación tanto a entidades establecidas en la UE como aquellas empresas que realicen tratamiento de datos que deriven de la oferta de bienes y servicios destinados a ciudadanos europeos, o como consecuencia de la monitorización de su comportamiento. Estas organizaciones deben designar un representante en la UE. Ello conlleva a que las multinacionales de Internet deban ajustarse a las previsiones de la normativa europea. [13]

Se introduce la figura del Delegado de Protección de Datos, como la persona encargada de informar a la entidad responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de supervisar el cumplimiento normativo al respecto. Además de cooperar con la autoridad de control y actuar como punto de contacto entre ésta y la entidad responsable del tratamiento de datos. [14]

En síntesis puede decirse que el RGPD propone un cambio importante de modelo de protección de datos en Europa basado en criterios como la responsabilidad activa (accountability), la flexibilidad, la importancia del contexto en el tratamiento de datos y la cooperación entre autoridades con competencia en esta materia. [15]

2. Panorama legal en España: evolución y adaptación al nuevo RGPD.

La Constitución Española, dispone en su artículo 18.4: "*La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*.

El artículo 18.4 CE se desarrolló por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), que derogaba

[13] PIÑAR MAÑAS, José Luis.; <<Introducción. Hacia un nuevo modelo…>>, cit., p.19
[14] Dossier: Manual de las principales novedades del Reglamento..., cit.
[15] ÁVAREZ HERNANDO, Javier, <<El Reglamento Europeo y la futura Ley General de Protección de Datos: sus principales novedades>>, Dossier: Manual de las principales novedades del REPD, 2018. pp 7-12, p 7.

la anterior Ley Orgánica 5/1992 de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal cuya regulación ya no se adaptaba a la realidad social.

En el panorama español destacan dos sentencias dictadas por el Tribunal Constitucional sobre el artículo 18.4 de la CE después de la entrada en vigor de la LOPD:

* La STC 94/1998, de 4 de mayo, que señaló que el derecho fundamental a la protección de datos garantiza a la persona el control sobre sus datos, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados. El derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquél que justificó su obtención.

* La STC 292/2000, de 30 de noviembre de 2000, que distinguió entre dos derechos: el derecho a la intimidad que permite excluir ciertos datos de una persona del conocimiento ajeno, es decir, el poder de resguardar su vida privada de una publicidad no querida; y el derecho a la protección de datos que garantiza a los individuos un poder de disposición sobre esos datos. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos datos que sean relevantes para o tengan incidencia en el ejercicio de cualquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado.[16]

Desde entonces, se ha puesto de manifiesto por la sociedad la preocupación por la protección de sus datos, necesidad que ha sido objeto de protección por el legislador europeo y español. Y no es para menos puesto que "el fundamento de la protección de datos protege originariamente la dignidad de la

[16] SERRANO CHAMORRO, Mª Eugenia, <<Protección de datos personales: información, consentimiento y transparencia. Nuevas exigencias jurídicas comunitarias>>, Actualidad Civil nº 5, 1 de mayo de 2017, Editorial Wolters Kluwer, p. 6

persona humana, constituye un ámbito de libertad del individuo, y tiene una concreción inexorable en los derechos clásicos de personalidad, como son el honor, la intimidad y la propia imagen"[17]

En España, la Agencia Española de Protección de Datos (AEPD) es la autoridad de control independiente que vela por el cumplimiento de la normativa sobre protección de datos y garantiza y tutela el derecho fundamental a la protección de datos personales.

La adaptación de nuestra legislación al Reglamento General de Protección de Datos ha hecho necesaria la elaboración de una nueva Ley Orgánica.

"Se atiende a nuevas circunstancias provocadas por el aumento de los flujos transfronterizos de los datos personales como consecuencia de la actividad del mercado interior, teniendo en cuenta que la rápida evolución tecnológica y la globalización han provocado que esos datos sean un recurso para la sociedad de la información. Todo ello ha determinado uno de los riesgos inherentes a que las informaciones sobre los individuos se hayan multiplicado de forma exponencial siendo más accesibles y más fáciles de procesar, al tiempo que se ha hecho más difícil el control de su uso y destino."[18]

Debido a ello, el Gobierno presentó el 24 de noviembre de 2017 el Proyecto de Ley Orgánica de Protección de Datos de carácter personal, actualmente –mayo de 2018- en fase de informe de la Comisión del Congreso.

[17] REBOLLO DELGADO, Lucrecio y SERRANO PEREZ, María Mercedes, *Manual de protección de datos*, Dykinson, 2014, p. 36

[18] "El Gobierno aprueba el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal". Diario La Ley. Editorial Wolters Kluwer. 10/11/2017.

III. ANÁLISIS DE LA PROTECCIÓN DE DATOS PERSONALES

1. El Derecho fundamental a la protección de datos personales. Evolución:

En la segunda mitad del siglo XX se entendió que el derecho a la intimidad era insuficiente para responder a los casos de violación de la dignidad de las personas, su libertad u otros derechos fundamentales por el tratamiento automatizado de la información personal en las nuevas tecnologías de aquel momento. Por ello, en los años setenta se tomó como objetivo el establecimiento de un nuevo derecho fundamental que diera cobertura a las nuevas demandas sociales.

En el continente europeo destacan por sus aportaciones los trabajos de VITTORIO FROSINI en los años 60 para quien "*la libertad informática consiste en el derecho de autotutela de la propia identidad informática: o sea el derecho de controlar (conocer, corregir, quitar o agregar) los datos personales inscritos en las tarjetas de un programa electrónico, pues lo que está en juego no es propiamente la intimidad de las personas, sino su propia identidad*"[19]

Destaca también en la consagración como un derecho fundamental autónomo la aportación jurisprudencial de la sentencia de 15 de diciembre de 1983 del Tribunal Federal Alemán en la cual se reconoció por primera vez el derecho a la autodeterminación informativa hasta ese momento invocado por la doctrina. El Tribunal Alemán configuró la facultad del individuo derivada de la idea de autodeterminación, de decidir por sí mismo cuándo y dentro de qué límites procedía revelar situaciones referentes a la propia vida. Se extrae del derecho al libre desarrollo de la personalidad la facultad de cada persona de disponer sobre la revelación y uso de sus datos, entendiendo el derecho a la autodeterminación informativa como la facultad general de disponer de los

[19]GARRIGA DOMÍNGUEZ, Ana, <<Nuevos retos para la Protección de Datos Personales: En la Era del Big Data y de la computación ubicua>>, Dykinson, Madrid, 2015, p. 92.

datos propios.[20] Esta sentencia puso de manifiesto que el peligro para las personas se encontraba, no en el carácter de los datos personales, sino en su utilización y posible aplicación, por lo que se consideró necesario la protección de los datos personales relativos a las personas mediante nuevos instrumentos jurídicos.

En España fue el Tribunal Constitucional (TC) el que tuvo que ir definiendo los principios y derechos que formarían el contenido esencial del derecho a la protección de datos personales. En 1993 el TC se pronunció sobre el alcance del derecho fundamental a la protección de datos personales, mediante la sentencia 254/1993 de 20 de julio. Esta resolución afirma que el artículo 18.4 CE consagra un derecho fundamental autónomo y diferente del de la intimidad.

Cuando el artículo 18.4 CE dispone que la Ley debe limitar el uso de la informática para garantizar la intimidad, el honor y el pleno ejercicio de los derechos de los ciudadanos está incorporando una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de las personas, un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama <<la informática>>."[21]

En la definición de lo que es y lo que comprende el ámbito del derecho fundamental de protección de datos tuvo también gran relevancia la ya citada Sentencia del Tribunal Constitucional 292/2000 de 30 de noviembre. Para una mayor protección de los individuos frente a injerencias por parte de poderes públicos, la misma sentencia del TC señala que la Constitución "impone a los poderes públicos la prohibición de que los individuos se conviertan en fuentes de información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan del acceso o divulgación indebidas de dicha información".

[20]GARRIGA DOMÍNGUEZ, Ana, <<Nuevos retos..., cit., p. 93.
[21]GARRIGA DOMÍNGUEZ, Ana, <<Nuevos retos..., cit., p. 95.

A estos límites fijados para la protección de datos personales se les ha denominado principios de calidad de los datos. [22]

Para finalizar con las sentencias que más influencia han tenido en nuestro país en la configuración del derecho de protección de datos, se debe resaltar la importancia de la STC 202/1999 de 8 de noviembre. En ella se refiere a los principios generales de la protección de datos y a la necesaria congruencia y racionalidad de los usos de la información personal.

El poder de disposición sobre los propios datos, que el derecho a la protección de datos personales garantiza, se lleva a cabo a través de un conjunto de facultades que formarían el denominado *habeas data* y que *"consistirán en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos"*. Este conjunto de facultades también forman parte del contenido esencial del derecho fundamental a la protección de datos personales[23].

2. Concepto de dato personal:

La definición de dato de carácter personal viene recogida en el art. 4.1 RGPD: "cualquier información numérica, alfabética gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables". Según jurisprudencia son datos personales: nombre, apellidos y dirección, DNI, datos de una solicitud de residencia; número de teléfono personal; la imagen; los datos de un registro de trabajo relativos a un trabajador; la dirección de correo electrónico; las direcciones IP.[24]

La Profesora SERRANO CHAMORRO, define datos personales en base a lo que establece el RGPD: <<*Un dato de carácter personal es cualquier*

[22]GARRIGA DOMÍNGUEZ, Ana, <<Nuevos retos..., cit., p. 98
[23]GARRIGA DOMÍNGUEZ, Ana, <<Nuevos retos..., cit., p. 98
[24] Dossier: Manual de las principales novedades…, cit.

información que permita identificarte o hacerte identificable. Se requiere la concurrencia de un doble elemento: la existencia de una información o dato, y que dicho dato pueda vincularse a una persona física o identificable. […] Cuando la ley habla de datos de carácter personal no solo hace referencia a nombre y apellidos de las personas, sino que, de manera muy amplia, incluye cualquier tipo de información (DNI, fotografías, videos, voz, huellas, etc.)>>[25] Añade dicha autora que toda la información personal que el consumidor y usuario de Internet vuelca en la Red no es sino parte de su personalidad.

El artículo 2 del RGPD establece que la normativa se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

El Proyecto de LOPD en tramitación parlamentaria determina el procedimiento a seguir en la protección de datos de personas fallecidas y de personas fallecidas con discapacidad.[26] Los herederos de una persona fallecida que acrediten tal condición podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión. Como excepción, los herederos no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. El albacea testamentario así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, el acceso a los datos personales de éste y, en su caso su rectificación o supresión.
En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

[25]SERRANO CHAMORRO, María Eugenia, <<Protección de datos personales: información, consentimiento y transparencia. Nuevas exigencias jurídicas comunitarias>>, Actualidad Civil n.º 5, mayo 2017, Editorial Wolters Kluwer, p. 6.
[26]SERRANO CHAMORRO, María Eugenia, <<Protección de datos personales...>>, cit., p. 7.

En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo.

3. El tratamiento del consentimiento:

3.1. Concepto:

El derecho fundamental a la protección de datos se sustenta sobre dos pilares reconocidos como tales por el Tribunal Constitucional: el consentimiento y los derechos de los interesados.[27]

El tratamiento de la información de carácter personal constituye una parte básica de las relaciones de la persona con el exterior, por lo que los ordenamientos jurídicos reconocen la posibilidad de que los individuos consientan y autoricen, de que puedan controlar la recogida y la utilización de la información personal.

Se afirma que consentir equivale a extender la capacidad de decisión de la persona con el fin de proteger su libertad y sus derechos en el mundo tecnológico.[28].

En el actual RGPD cobra gran importancia la regulación del consentimiento, artículo 4.11. Supone toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. La novedad que introduce esta regulación radica en que se especifican las formas de expresar el consentimiento, que puede ser mediante una declaración, y mediante una acción.
Para el RGPD el consentimiento debe darse mediante un acto afirmativo claro

[27]REBOLLO DELGADO, Lucrecio y SERRANO PEREZ, Maria Mercedes, *Manual..., cit., p.* 112
[28]SERRANO CHAMORRO, María Eugenia., <<Protección de datos personales…>>, cit., p. 11

que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como: una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir: marcar una casilla de un sitio web en Internet, escoger parámetros técnicos (cookies), para la utilización de servicios de la sociedad de la información o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales.

Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento.

Respecto al consentimiento el RGPD indica que éste debe darse para todas y cada una de las actividades de tratamiento realizadas con el mismo o los mismos fines.

Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta. El silencio o la inacción no podrán ser considerados como una declaración del consentimiento, que sólo se dará con un acto afirmativo claro y para unos fines específicos.[29]

3. 2. Licitud del tratamiento y condiciones del consentimiento

El artículo 6 RGPD recoge los casos en que será lícito el tratamiento de datos personales si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

[29]SERRANO CHAMORRO, María Eugenia., <<Protección de datos personales...>>, cit., p. 11.

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

En el apartado 4 del mismo artículo se ofrecen los criterios para determinar si el consentimiento ha sido realmente libre o se ha impuesto al usuario el tratamiento de datos que no son necesarios para la prestación de un servicio.

En los apartados 1 y 2 del artículo 7 se establecen la prueba de que éste realmente se dio, y que se dio cumpliendo las condiciones esenciales que debe tener para que se considere válido: "*Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.*"[30]

En el RGPD se contempla la posibilidad de que se retire o se revoque el consentimiento ya que se ha consagrado como un principio la revocación el consentimiento del interesado, por lo que será tan fácil retirar el consentimiento como darlo.

[30] ADSUARA VARELA, Borja, <<El consentimiento>>…, cit., p. 165.

3.3 El consentimiento del menor:

Debido a la expansión de la tecnología digital, el legislador ha decidido dar una protección específica al uso de la tecnología por menores, y también por los adultos cuando traten con niños, (art. 8 RGPD).

En primer lugar se establece que cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años.[31]

Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años, estableciéndose de esta manera un mínimo que deben cumplir todos los países miembros cuando regulen este aspecto de la protección de datos.

Se consagran como premisas de gran importancia para la protección de los niños: el establecimiento de la edad mínima de 13 años, por debajo de la cual los países miembros no podrán establecer como lícito el consentimiento, y, que si el niño es menor de 16 años sólo será lícito si dicho consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, siendo ésta necesaria en todo caso sin contemplarse ningún tipo de excepción. [32]

Destaca el cambio que se ha introducido puesto que el anterior Reglamento español de la LOPD disponía que podía concederse el tratamiento de los datos de los mayores de 14 años con su consentimiento.

[31] ADSUARA VARELA, Borja., <<El consentimiento>>…, cit., p. 165.
[32] ADSUARA VARELA, Borja., <<El consentimiento>>…, cit., p. 165.

El RGPD determina que el responsable del tratamiento realice esfuerzos razonables para verificar que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.

Sin embargo, en el Reglamento de la LOPD se exigía una mayor responsabilidad al responsable del fichero o tratamiento porque le pedía articular los procedimientos que garantizasen que se había comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado, en su caso, por los padres, tutores o representantes legales.[33]

El RGPD hace hincapié en que es particularmente importante la protección de los datos de los menores en el caso de los servicios de la sociedad de la información ofrecidos directamente a un menor y cuando sus datos se utilizan con fines de marketing y creación de perfiles online. [34]

3.4. Categorías especiales de datos personales:

El RGPD trata también categorías especiales de datos personales, prohibiendo el tratamiento de datos personales que revelen: el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical. Se trata de que no se pueda dar ningún tipo de dato personal que pueda inducir de manera indirecta a discriminación. Además prohíbe el tratamiento de: datos genéticos, datos biomédicos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación(es) sexuales de una persona física.
El artículo 9 RGPD describe una serie de circunstancias para las que no será de aplicación la prohibición de tratamiento de las categorías especiales de datos personales, como: si el interesado dio su consentimiento explícito para el tratamiento de sus datos con algún fin especificado; o sea preciso respecto a

[33] ADSUARA VARELA, Borja, <<El consentimiento>>…, cit., p. 165.
[34] https://www.itgovernance.eu/blog/es/rgpd-proteccion-de-datos-consentimiento-y-menores-de-edad [fecha de consulta 20/04/2018]

obligaciones de Derecho Laboral y de la Seguridad Social; o el tratamiento se necesite para protección vital del interesado o de terceras personas; o el tratamiento se realice por entidades sin ánimo de lucro con fines políticos, filosóficos, religiosos o sindicales; o el interesado ya haya hecho manifiestamente públicos sus datos personales; u otros tratamientos relacionados con la preeminencia de intereses públicos esenciales, el ejercicio del poder judicial o de prevención de riesgos laborales, entre otros.

Del listado de categorías especiales de datos personales, el RGPG regula por primera vez dos de las categorías: datos genéticos y datos biomédicos dirigidos a identificar de manera unívoca a una persona física.

También es novedad que aunque estas categorías especiales de datos pueden ser tratadas con consentimiento explícito del interesado, se prevé que el Derecho de la Unión o de los Estados miembros puedan impedir que el interesado lo preste[35].

V. EL DELEGADO DE PROTECCIÓN DE DATOS

1. La nueva figura jurídica: el Delegado de Protección de Datos:

1.1. La incorporación del DPO en la protección de datos personales:

El RGPD ha introducido en España una nueva figura jurídica: el Delegado de Protección de Datos, en inglés *Data Protection Officer* (DPO).

El DPO es considerado como una figura consustancial al propio derecho a la protección de datos personales. Es una figura requerida para una protección plena y efectiva de la persona en lo que respecta al tratamiento de sus datos

[35] ADSUARA VARELA, Borja, <<El Consentimiento>>…, cit., p. 167.

personales. Además, ambién se les considera clave en generar e impulsar la confianza necesaria para el desarrollo de una economía digital robusta.[36]

Para llevar a cabo sus funciones el DPO ha de tener garantizada su independencia. Esta obligación corresponde a los responsables y encargados del tratamiento, que a su vez son los encargados de la designación de los DPO en los casos previstos en el Reglamento, o cuando decida designarse esta figura voluntariamente.

El origen del DPO surge en la legislación alemana, ya que fue este país el primero en incorporar esta figura jurídica en su Ley Federal de protección.

En el ámbito europeo el DPO fue introducido a través de una enmienda realizada a la propuesta de Directiva 95/46/CE, y más tarde Francia, Suecia, Luxemburgo o los Países bajos consideraron que tal figura podía aportar cambios positivos en la protección de datos personales, adoptándola en sus respectivos ordenamientos jurídicos.

Más países fueron poco a poco incluyendo en sus ordenamientos esta posibilidad, incluso existían DPO en el ámbito de instituciones y organismos comunitarios en virtud del Reglamento nº 45/2001 del Parlamento Europeo y del Consejo relativo a la protección de personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

El Tribunal de Justicia de la Unión Europea se pronunció sobre esta figura en la sentencia dictada en 2010 para el caso *Volker und Markus Schecke y Eifert*.
En esta STJUE se resaltaba la importancia del DPO: "le incumbe ejecutar diversas tareas destinadas a garantizar que el tratamiento de los datos no pueda ocasionar una merma de los derechos y libertades de los interesados".

[36] RECIO GAYO, Miguel, <<El delegado de protección de datos>>, en María Álvarez Caro y Miguel Recio Gayo (coord.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*, Editorial Reus, Madrid, 2016, pp. 367-388, en p. 368.

1.2. Definición y características del Delegado de Protección de Datos:

"El Delegado de Protección de Datos es una persona responsable, en el seno de un responsable del tratamiento o un encargado del tratamiento, de supervisar y monitorear de manera independiente la aplicación interna y el respecto de las normas sobre protección de datos…"[37]

Se ha establecido la posibilidad de que pueda ser un empleado de la misma empresa en el seno de la cual trabaja, o ser un consultor externo a esta.

El mismo será designado en base a sus cualidades profesionales, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas para ellos en el Reglamento.

Los conocimientos que posean los Delegados deben haber sido adquiridos a través de una formación homologada, puesto que la posición que ocupan es de gran relevancia al velar por un derecho fundamental. Estos conocimientos se consideran imprescindibles para poder identificar los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento; tal y como expresa el art. 39.2 del Reglamento.

La necesidad de formación específica del DPO radica en el hecho de que se esté ante un derecho fundamental y de que el mismo tiene un relevante papel al evaluar si un tratamiento de datos puede ocasionar una merma del mismo.[38]

Uno de los aspectos a los que más importancia se le da en el Reglamento es la especial posición del DPO en la práctica diaria de las empresas que traten con datos personales. Es clave en el aseguramiento de la gobernanza de la organización en relación al derecho fundamental de protección de datos. Por

[37] RECIO GAYO, Miguel, <<El delegado de protección de datos>>…, cit., p. 375.
[38] RECIO GAYO, Miguel, <<El delegado de protección de datos>>…, cit., p. 376.

ello se establece la necesidad de garantizar que se le proporcionen a los DPO los recursos necesarios para que desarrollen sus funciones, y para que además las desempeñe de manera independiente. También se ha regulado su protección ante despidos o sanciones por el desempeño normal de su trabajo.

El DPO tiene que estar en una posición mediante la cual sea fácil tener una comunicación efectiva con todos los interesados cuyos datos personales tratan en esa determinada empresa. Y, a su vez, una posición que le permita cooperar con las autoridades de control.

El Supervisor Europeo de Protección de Datos se pronunció al respecto de la independencia y de la importancia de garantizarla explicando que para que nadie interfiera en el desempeño de sus funciones, los Delegados de Protección de Datos no recibirán instrucciones de superiores, debiendo reportar sólo a la autoridad que le designó para el puesto. [39]

Los DPO no podrán ser destituidos ni sancionados por el responsable o el encargado por desempeñar sus funciones.

La posición del DPO tiene que permitirle desempeñar sus funciones de manera independiente, a través de una comunicación efectiva con las partes interesadas, y también de manera que pueda contribuir a desarrollar el nuevo marco de gobernanza de datos que establece el Reglamento, y que se basa fundamentalmente en el principio de responsabilidad.[40]

1.3. Funciones y designación del Delegado de Protección de Datos:

Se concretan en el artículo 39 del RGPD las funciones que, como mínimo, tendrán los Delegados. Se trata de una lista abierta siendo en cada caso adaptada a cada trabajo que realice.

[39] RECIO GAYO, MIGUEL., <<El delegado de protección de datos>>, cit., p.375.
[40] RECIO GAYO, MIGUEL., <<El delegado de protección de datos>>, cit., p. 385.

Las funciones son:

1. Información y asesoramiento: Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en;
2. Supervisión del cumplimiento, asignación de responsabilidades, concienciación y formación del personal;
3. Asesoramiento sobre la evaluación de impacto sobre protección de datos: ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con la ley;
4. Cooperación con la autoridad de control;
5. Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento.

Para realizar las funciones establecidas en este artículo, es necesario que los Delegados sean designados de la forma concreta que se establece en el RGPD, y por las personas encargadas legalmente para ello.[41]

En base al artículo 37 RGPD tienen la obligación de designar o nombrar a un DPO los responsables o encargados del tratamiento en los siguientes casos:

– Artículo 37. 1.a): Administraciones Públicas: el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
– Artículo 37. 1.b); c); y 37.4: Responsable o encargado del tratamiento en el sector privado cuando:

a) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala;

b) o las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales.

[41] RECIO GAYO, Miguel, <<El delegado de protección de datos>>…, cit., p.375.

En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros. El DPO podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados.

En el caso de las autoridades u organismos públicos con independencia de los datos personales que traten y de que actúen como responsables o encargados del tratamiento, el artículo 37.3 del Reglamento prevé que éstas puedan designar un único DPO para varias de estas autoridades u único DPO para varias de estas autoridades u organismos teniendo en cuenta su estructura organizativa y tamaño.[42]

Los grupos de empresas también podrán designar a un único DPO para todo el grupo de empresas si es fácilmente accesible desde cada establecimiento.

Una vez designado el responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

En cuanto al DPO en España, se debe señalar que la Agencia Española de Protección de Datos ha puesto en marcha en su sede electrónica un procedimiento para que las Administraciones públicas y las entidades privadas obligadas a designar un DPO puedan comunicar este nombramiento, tal y como se establece en el nuevo RGPD. Este nuevo procedimiento para la comunicación del DPO es un formulario online al que se accede con certificado electrónico.

Este sistema de notificación electrónica no se circunscribe únicamente a las Administraciones Públicas y a las entidades privadas obligadas. Las empresas

[42] RECIO GAYO, Miguel, <<El delegado de protección de datos>>, …cit, p. 379.

que no estén obligadas por las previsiones del Reglamento a designar un DPO y que quieran implantar esta figura en sus organizaciones como apoyo al cumplimiento pueden utilizar este formulario con el fin de comunicarlo.[43]

2. Figuras afines al Delegado de Protección de Datos:

El DPO puede ser designado como parte de un equipo de profesionales, si se considera positivo para el funcionamiento de la organización, compuesto por:

El Compliance Officer:

La figura del Delegado de Cumplimiento normativo o Compliance Officer se desarrolló por la Directiva 2004/39/CE, del Parlamento Europeo y del Consejo, de 21 de abril de 2004, de Mercado de Instrumentos Financieros.

Se define como el agente, designado por la empresa, que integrante o no de la propia organización, y con poderes autónomos de iniciativa y control, realiza una función de asistencia al órgano de administración y dirección de la persona jurídica u organización públicas y privadas en el cumplimiento de la legalidad vigente, asesorando en la identificación e implantación de controles así como monitorizando la efectividad de los mismos.
Su principal tarea consiste en la prevención de delitos contemplados en el artículo 31 bis CP, detectarlos y reaccionar frente a ellos.[44]

Los principios que deben regir a estos profesionales son los siguientes[45]:

- Actuar de forma honesta, imparcial y profesional en el mejor interés de sus clientes.
- Proporcionar información imparcial, clara y no engañosa a sus clientes.

---

43 http://www.agpd.es/portalwebAGPD/revista_prensa [fecha de consulta: 10/04/2018]

44 BELÉN LINARES, María, <<Programas penales de cumplimiento en el seno de la persona jurídica tras la LO 1/2015>>, La Ley Penal nº 118 enero-febrero 2016, Ed. Wolters Kluwer.

45 ALARCÓN GARRIDO, Antonio, Manual teórico-práctico del Compliance Officer, Sepin, Madrid, 2016, p. 37.

- Prestar servicios y ofrecer productos teniendo en cuenta las circunstancias personales de los clientes.

Actualmente, la profesión no tiene un marco normativo propio que regule el acceso y el ejercicio del cargo. Aunque existen algunas asociaciones sobre cumplimiento normativo como "Cumplen" o "Ascom". La primera de ellas ha elaborado un Estatuto General de la Profesión de Compliance Officer[46] que establece que: “es un Compliance Officer quien, estando en posesión del título oficial de Licenciado en Derecho, en Dirección de Administración y Dirección de empresa, o con titulación análoga o experiencia equivalente, se dedica de forma profesional a realizar los actos propios de la profesión, bien de manera individualizada, o incorporado a una sociedad profesional, o prestando servicios en concepto de tal a una entidad o persona jurídica pública o privada”.

Responsable del fichero o del tratamiento:

Sería la persona física o jurídica de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento de datos, aunque no lo realizase materialmente.

Pueden ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados; así de acuerdo con la STJUE 13-5-14, asunto Google Spain, los motores de búsqueda pueden ser responsables del tratamiento de datos personales.[47]

Las finalidades se encuentran recogidas en la normativa, y es posible que el tratamiento tenga varios fines, siempre que sean específicos, pues así lo establece el artículo 6 RGPD:

[46] https://www.cumplen.com/recursos/archivos/Estatuto-Profesional-del-Compliance-2.pdf [fecha de consulta: 04/04/2018]

[47] LÓPEZ ÁLVAREZ, Luis Felipe, *Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo,* Francis Lefebvre, Madrid, 2016, p. 26.

De manera individual se recogen unas finalidades vinculadas a intereses públicos:

- El cumplimiento de obligaciones legales del responsable;
- La protección de intereses vitales de las personas físicas;
- Cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable de tratamiento.

De forma más genérica se recogen las siguientes dos finalidades. Se refieren más a entidades privadas:
a) La satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero;
b) La contratación y su ejecución posterior o aplicación de medidas precontractuales. [48]

Además el artículo 24 del RGPD fija las obligaciones fundamentales del responsable indicando que está obligado a adoptar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento se realiza conforme al Reglamento.[49]

Encargado del Tratamiento:

Es la persona física o jurídica, autoridad pública, servicio u otro organismo que trata datos personales por cuenta del responsable del tratamiento. Es una institución que permite conceder acceso a los datos de aquellos prestadores de servicios que así lo precisen, en la medida en que los tratamientos se realicen por cuenta del responsable. [50]

Se considera que se creó una ficción por la cual se entiende que los datos no son revelados a un tercero, sino que permanecen bajo la esfera de control del

[48] LÓPEZ ÁLVAREZ, Luis Felipe, *Protección de datos personales…,* cit., p. 33.
[49] LÓPEZ ÁLVAREZ, Luis Felipe, *Protección de datos personales…,* cit., p. 121.
[50] NÚÑEZ GARCÍA, José Leandro, <<El encargado de tratamiento>>, en María Álvarez Caro y Miguel Recio Caro (coord.), Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad, Editorial Reus, Madrid, 2016, pp. 321-333, p. 322.

propio responsable, a pesar de que sean gestionados por una tercera entidad.[51] El elemento definidor del responsable reside en su capacidad de decisión para determinar los fines y los medios del tratamiento, el encargado se caracteriza por encontrarse sometido a las decisiones del primero. Se basa en una delegación de funciones en una organización externa, jurídicamente diferenciada, que tratará los datos en nombre y por cuenta de aquél que requiere sus servicios.[52]

3. Responsabilidad: penal, administrativa, y civil.

Debido a la gran relevancia que tienen los responsables de tratamiento de datos personales, el RGPD ha regulado un amplio marco de deberes que deben cumplir en el desarrollo del tratamiento de datos personales. Las responsabilidades en que pueden incurrir en la realización de sus funciones, se encuadran en el ámbito penal, civil y administrativo.
El primer ámbito sobre los ilícitos penales; el segundo, sobre la necesidad de indemnizar los daños y perjuicios causados; y, el tercero, sobre la responsabilidad ante las infracciones administrativas.

El artículo 22 del RGPD establece que toda persona debe disponer de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, sin perjuicio del recurso administrativo que pueda interponerse, en particular ante la autoridad de control y antes de acudir a la autoridad judicial.

Además, el artículo 79 establece el Derecho a la tutela judicial efectiva contra un responsable o encargado de tratamiento: "todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de datos personales".

---

[51] En la misma línea, PIÑAR MAÑAS, José Luis, <<Novedades en relación con la figura del encargado del tratamiento>>. Publicado en ZABÍA DE LA MALTA, Juan (Coord.) Protección de Datos: Comentarios al Reglamento, Ed. Lex. Nova, Valladolid, 2008, p. 219.

[52] NÚÑEZ GARCÍA, José Leandro, <<El encargado de tratamiento>>,…,cit., p. 322.

Estas acciones se ejercitarán ante los Tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento, o alternativamente ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos.[53]

El Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal contempla como sujetos responsables sometidos al régimen sancionador a: los responsables de los tratamientos; los encargados de los tratamientos; los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea; las entidades de certificación; las entidades acreditadas de supervisión de los códigos de conducta. Se excluye expresamente su aplicación a los DPO.

1. Responsabilidad Penal:

La responsabilidad penal se recoge principalmente en el artículo 197 CP.

En este artículo, en su apartado primero se establecen condenas de prisión de uno a cuatro años, y multas de doce a veinticuatro meses con carácter general para quienes descubran los secretos o vulneren la intimidad del interesado sin su consentimiento. En el presupuesto de alguna de las acciones contempladas por artículo del CP pueden tener encaje los accesos indebidos a datos personales como medio para introducirse, por ejemplo, en la cuenta de correo electrónico de la víctima.

El apartado 2 del artículo 197 establece las mismas penas para quienes se apoderen, utilicen o modifiquen, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.

[53] LÓPEZ ÁLVAREZ, Luis Felipe, <<La responsabilidad del responsable>>…, cit., p. 277.

Se impondrán las mismas penas a quienes accedan por cualquier medio a los ficheros y soportes anteriores a quienes los alteren o utilicen en perjuicio del titular de los datos o de un tercero, sin autorización.

Para incurrir en este tipo de responsabilidad, es necesaria la existencia de dolo, pues se requiere el ánimo de vulnerar la privacidad, apoderarse de información, utilizarla o modificarla en perjuicio de tercero. Es decir, se está ante acciones que llevan consigo un ánimo o intención dañosa.[54]

Lo mismo cabe indicar de otro tipo de acciones que pueden ser cometidas de forma imprudente, como apoderarse del correo o acceder por error o sin advertencia a los ficheros y soportes que contengan información de terceros. Resulta necesario comprobar que dicho acceso ha sido con la finalidad de aprovecharse de esa información para causar daños al titular de los datos o a un tercero, o cuanto menos, beneficiarse de la información. De esta forma el acceso accidental a la información por error o, porque el responsable del tratamiento no ha adoptado las medidas de protección oportunas no darán lugar a responsabilidad criminal, sin perjuicio de la administrativa en la que pueda incurrir. [55]

El artículo 197 apartado tercero, aumenta la pena hasta cinco años de prisión si se difunden, revelan o ceden a terceros los datos o hechos descubiertos, o las imágenes que se han obtenido mediante las acciones anteriores. Estas acciones ilícitas llevan aparejados daños para la víctima.

Los delitos que hemos mencionado pueden ser realizados por ciberdelincuentes. Pero también por los responsables y encargados de una actividad de tratamiento para los cuales aumenta la pena de prisión hasta cinco años si, quien realiza las conductas que se reconocen por los apartados 1 y 2, es responsable o encargado del tratamiento. Y cuando los datos se hayan difundido, cedido o revelado a terceros, las penas se impondrán en su mitad

[54] LÓPEZ ÁLVAREZ, Luis Felipe, <<La responsabilidad del responsable>>…, cit., p. 277.
[55] LÓPEZ ÁLVAREZ, Luis Felipe <<La responsabilidad del responsable>>…, cit., p. 278.

superior. Sin embargo, si no ha existido cesión o difusión de los datos, se imponen las mismas penas si se trata de datos especialmente protegidos. Si además de esta intención lucrativa se tratan datos especialmente protegidos o de menores o personas con discapacidad, entonces la pena aumenta significativamente debiéndose imponer de cuatro a siete años de prisión, además de multa de doce a veinticuatro meses en su mitad superior.

Estos mismos hechos pueden ser llevados a cabo por las autoridades y el personal al servicio de las Administraciones Públicas, en cuyo caso, la imposición de las condenas anteriores se establece en la mitad superior.

El artículo 197 bis extiende la protección penal contra quienes por cualquier medio o procedimiento, vulnerando las medidas de seguridad, y sin autorización, facilite a otro el acceso al conjunto o una parte del sistema de información, con una pena de prisión de seis meses a dos años.

Cuando es una empresa la que incurre en alguno de los supuestos previstos por el artículo 197, se le impondrá pena de multa de seis meses a dos años y los jueces y tribunales podrán asimismo imponer penas entre las que se encuentra la disolución de la persona jurídica o la clausura de sus locales.

Se deben destacar los supuestos en que las empresas de "cloud" o que prestan sus servicios en la nube no borren los datos de un cliente para el que han dejado de prestar servicios. Para estas empresas es esencial la figura del DPO, y la adopción de protocolos de *compliance* para poder prevenir la apertura de un procedimiento penal y la responsabilidad penal de la persona jurídica.[56]

La Reforma del Código Penal tras la Ley Orgánica 1/2015 de 30 de marzo, conllevó la inclusión en el mismo de ciertos delitos informáticos. El artículo 197 CP se modificó de la manera que sigue:[57]

[56] LÓPEZ ÁLVAREZ, Luis Felipe, <<La responsabilidad del responsable>>... cit., p. 279.

[57] http://www.legaltoday.com/practica-juridica/penal/penal/los-nuevos-delitos-informaticos-tras-la-reforma-del-codigo-penal [fecha de consulta: 01/05/2018]

Se introdujo la colaboración en el delito de intrusión informática por el que se facilita a un tercero el acceso a un sistema informático. La interceptación de transmisiones de datos informáticos fue una figura creada *ex novo*, mediante la cual se protege la seguridad de los sistemas informáticos. Se introdujo también la producción o facilitación a terceros de datos para la realización de los delitos anteriores, con el supuesto de agravación por actuar en el seno de una organización o grupo criminal. Además, se modificó el art. 197 CP para introducir la responsabilidad penal de la persona jurídica.

2. **Responsabilidad administrativa:**

En el Considerando 152 del RGPD se establece que en los casos en que el mismo no armonice las sanciones administrativas, o en otros casos en que se requiera, por ejemplo en casos de infracciones graves del presente Reglamento, los Estados miembros deben aplicar un sistema que establezca sanciones efectivas, proporcionadas y disuasorias. La naturaleza de dichas sanciones, ya sea penal o administrativa, debe ser determinada por el Derecho de los Estados miembros.

El artículo 83 del RGPD establece las condiciones generales para la imposición de multas administrativas. El mismo establece que cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, el mismo podrá aplicarse de tal modo que la incoación del procedimiento sancionador corresponda a la autoridad de control competente y su imposición a los tribunales nacionales competentes.

Pueden imponerse multas administrativas de 10.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior para los casos establecidos en el apartado 4 del mismo artículo, o hasta 20.000.000 en los casos establecidos en el apartado 5, optándose en ambos casos por la de mayor cuantía.

En el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal se contempla el régimen sancionador en los arts. 70 y siguientes. Se prevén infracciones leves, infracciones consideradas graves, e infracciones consideradas muy graves.[58] Se consideran leves y prescribirán al año las infracciones contenidas en el art. 74 de la que será la nueva LOPD. Se consideran infracciones graves y prescribirán a los dos años las contenidas en el art. 73 de la Ley Orgánica.
Se consideran infracciones muy graves las establecidas en el art. 72, las cuales prescribirán a los tres años.

El Proyecto de la LOPD establece en el artículo 77 el régimen aplicable a determinadas categorías de responsables o encargados del tratamiento, entre los que se encuentran:
a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
b) Los órganos jurisdiccionales.
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.
e) Las autoridades administrativas independientes.
f) El Banco de España.
g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
h) Las fundaciones del sector público.
i) Las Universidades Públicas.
j) Los Consorcios.
Cuando los responsables o encargados citados cometiesen alguna de las infracciones a las que se refieren los artículos 73 a 75, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La autoridad de protección de datos podrá proponer también la iniciación de actuaciones disciplinarias. Las resoluciones

[58] LÓPEZ ÁLVAREZ, Luis Felipe, <<La responsabilidad del responsable>>..., cit., p. 279.

que recaigan en relación con las medidas y actuaciones anteriores deberán ser comunicadas a la autoridad de protección de datos.[59]

Cuando la autoridad competente sea la Agencia Española de Protección de Datos, ésta publicará en su página web con la debida separación las resoluciones en que se imponga una sanción a estas entidades, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Hay que destacar como novedad introducida por el RGPD que ya no será sancionable la ausencia de solicitud de inscripción de los ficheros en la AEPD. En el artículo 24 y el considerando 89 del RGPD hacen depender de la exigencia de obtener autorización previa a determinados tratamientos que conlleven un alto riesgo para los derechos y libertades de las personas físicas.[60]

El considerando 90 del RGPD establece:
"El responsable debe llevar a cabo, antes del tratamiento, una evaluación de impacto relativa a la protección de datos con el fin de valorar la particular gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo. Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el presente Reglamento. ‘‘

3. Responsabilidad civil:

Las responsabilidades penal y administrativa se encuentran íntimamente unidas a la tercera, la civil, pues, aunque ésta tiene su propia autonomía de forma que puede surgir con independencia de no haberse vulnerado ninguna

[59] LÓPEZ ÁLVAREZ, Luis Felipe, <<La responsabilidad del responsable>>..., cit., p. 280.
[60] LÓPEZ ÁLVAREZ, Luis Felipe, <<La responsabilidad del responsable>>..., cit., p. 280.

norma penal o administrativa, cuando existe infracción queda demostrada la exigencia de dolo o culpa, requisito necesario para que surja el deber de indemnizar en vía civil por los daños o perjuicios causados al interesado.[61]

Se ha establecido el deber general del responsable o el encargado del tratamiento de indemnizar cualesquiera daños y perjuicios que pueda sufrir una persona como consecuencia de un tratamiento realizado en infracción del RGPD, en su considerando 146.

Existen dos esferas de responsabilidad: la que se deriva del incumplimiento del Reglamento que automáticamente provoca el deber de indemnizar el daño; y la que consiste en poder demostrar la ausencia de responsabilidad en el hecho que haya causado los daños y perjuicios. La carga de la prueba en este ámbito recae sobre el responsable, que deberá demostrar que su conducta ha sido diligente. Quien reclama el daño no tendrá que demostrar la culpa o negligencia del causante del daño.

En cuanto a la obligación de adoptar medidas, éstas deben ser proporcionales al riesgo que genera el tratamiento. Cuando la evaluación de impacto muestre que las operaciones de tratamiento suponen un alto riesgo que el responsable no puede mitigar es necesario que consulte a la autoridad de control, la cual dispondrá las medidas necesarias para reparar el daño. Como en estos casos no se elimina el riesgo, se asume la probabilidad de generación de daños.

Cuando el responsable del tratamiento sea una Administración Pública la responsabilidad será objetiva, pues así lo dispone la Constitución Española en el art. 106.2. Aunque la conducta se ajuste al reglamento, esto no impide que surja el deber de indemnizar, ya que es suficiente con demostrar que el daño ha sido causado por el funcionamiento o la actuación de la Administración para tener que indemnizar los daños causados. Por lo que no será necesario demostrar la existencia de dolo o negligencia en la acción que causa el daño.[62]

[61] LÓPEZ ÁLVAREZ, Luis Felipe, <<La responsabilidad del responsable>>..., cit., p. 280.
[62] LÓPEZ ÁLVAREZ, Luis Felipe <<La responsabilidad del responsable>>…, cit., p. 280-282.

El régimen de responsabilidad patrimonial de las Administraciones Públicas se expone en el Capítulo IV, del Título Preliminar de la Ley 40/2015 Ley del Régimen Jurídico del Sector Público, artículos 32 y siguientes.
Los requisitos generales para apreciar la concurrencia de la responsabilidad patrimonial se encuentra en los apartados 1º y 2º de la LRJSP.

En consecuencia, para apreciar un supuesto de responsabilidad patrimonial de la Administración deberán concurrir los requisitos determinados tanto en vía legal como en la jurisprudencial. Estos requisitos son:

a) Que haya generado un daño real y efectivo, evaluable económicamente e individualizado.
b) Que se trate de relación directa, inmediata y exclusiva de causa-efecto, sin la concurrencia de circunstancias que puedan enervar el nexo causal, tales como la fuerza mayor o la conducta propia del perjudicado.
c) La antijuridicidad de la lesión, entendida como la ausencia de la obligación de soportar el referido daño por parte del ciudadano.
e) Que la reclamación se efectúe en el plazo de un año desde que se ocasionó el citado daño.[63]

[63] https://www.notariosyregistradores.com/web/secciones/doctrina/articulosdoctrina/responsabilidad -patrimonial-administracion/ [fecha de consulta: 21/04/2018]

VI. CONCLUSIONES:

PRIMERA. Con el Reglamento General de Protección de Datos se ha puesto fin al proceso unificador de la legislación de protección de datos personales en la UE, y a su vez se ha adaptado la norma en este ámbito a los nuevos riesgos y necesidades sociales, para favorecer el mercado interior. Además, en nuestro país, ha supuesto la tramitación de una nueva Ley Orgánica de Protección de Datos para ajustar nuestro ordenamiento jurídico a las nuevas directrices. Con ello se pretende dar la mayor cobertura posible al derecho fundamental a la protección de datos.

SEGUNDA. El Reglamento Europeo establece que el consentimiento para tratar datos personales con carácter general sea libre, informado, específico e inequívoco, es decir, debe prestarse mediante una acción positiva del interesado, por lo que no será válido el consentimiento tácito como ocurría con anterioridad. Para los datos sensibles se requiere un consentimiento explícito. Lo que supone que la declaración se refiera de forma específica al consentimiento y tratamiento en cuestión. El mismo debe ser verificable.

TERCERA. El Reglamento configura la información como un derecho de los afectados y diferencia los derechos a la rectificación y la supresión -derecho al olvido-. El derecho de oposición forma parte del derecho de supresión, y se crean dos nuevos derechos: el de limitación y el de portabilidad.

CUARTA. Se regulan las condiciones aplicables al consentimiento del menor en relación con los servicios de la sociedad de la información. Si el menor tiene menos de 16 años el tratamiento de sus datos personales se considerará lícito sólo si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela del niño. También se establece que el tratamiento de datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de 13 años, fijando esta edad como edad mínima que todos los países deben acatar.

QUINTA. El Proyecto de la nueva LOPD incorpora una novedosa regulación de los datos referidos a las personas fallecidas. Se permite que los herederos puedan solicitar el acceso a los mismos, rectificarlos, e incluso suprimirlos.

SEXTA. Se incorpora la figura del Delegado de Protección de Datos, persona encargada de informar a la entidad responsable o al encargado del tratamiento sus obligaciones legales en materia de protección de datos. Esta figura jurídica es una nueva opción de trabajo con futuro para los graduados en Derecho. Para acceder a ser DPO se tendrán en cuenta sus cualidades profesionales, en particular sus conocimientos especializados del Derecho, la práctica en materia de protección de datos personales, y su capacidad para desempeñar las funciones de responsabilidad inherentes a dicho cargo.

SÉPTIMA. El Compliance Officer se encarga, como principal tarea, de la prevención de delitos, de la detección de los mismos y reaccionar frente a los mismos. Mientras que el Delegado de Protección de Datos o Data Protection Officer se encargaba de informar a la entidad responsable o al encargado del tratamiento sus obligaciones legales en materia de protección de datos.

OCTAVA. Las responsabilidades en que pueden incurrir los responsables de tratamientos de datos personales se pueden encuadrar en el ámbito penal, civil y administrativo. La futura Ley Orgánica de Protección de Datos regula el régimen sancionar, en el cual se prevén infracciones leves, infracciones graves e infracciones muy graves.

VII. EXTENDED SUMMARY.

THE DATA PROTECTION OFFICER FIGURE AND PRIVACY PROTECTION

The 1950 European Convention of Human Rights recognized for the first time the right to data protection, and the 1981 Council of Europe Convention for people's protection with respect to the automatic processing of personal data, was the first legal, binding instrument in the issue of data protection.

European Union member States regulated the right to data protection by means of their own instruments, fact which broached the lack of uniformity in the matter, and the hampering of the EU's internal market.
By virtue of this fact, an legal instrument endemic to EU in terms of data protection was adopted, the Directive No. 95/46/EC of the European Parliament and the Council of 24th October 1995, which has implied the foundation for the current statutory regulation of the General Data Protection Regulation (GDPR), which will be applicable from the 25th of May 2018.

In this way, a reduction of legal fragmentation of the member States began to be achieved, and therefore, a higher legal certainty.

The object of the General Data Protection Regulation is double, inasmuch as it regulates the right to personal data processing and, simultaneously, it guarantees the free movement of data.

The GDPR includes the following innovations:

1. definitive consolidation of data processing as a fundamental right
2. definition and legal regulation of consent
3. regulation of the "right to be forgotten"
4. regulation of the new "right to data portability"
5. incorporation of the principle of Proactive Responsibility

6. demand of a default consideration of the Privacy principles from the very first design perspective
7. lack of need of file registration
8. obligation of notifying security breaches
9. regulation of impact assessments relative to data protection
10. previous-to-processing consultation, if the processing entails a high risk
11. enhancing creation and development of certification, stamp and trademark mechanisms for data protection
12. regulation of international transfers with an explicit reference to the corporative, binding rules as transfer legitimization
13. the independent-to-control authorities regime and the cooperation and coherence mechanism
14. new regulation of the European Council of Data Protection
15. appeals, responsibilities and penalties regime

The GDPR is applicable both to established entities in the EU and to those companies conducting the processing of data deriving from the offer of goods and services addressed to European citizens. These organizations must designate a legal representative in the EU.

The consent to process personal data must be free, informed, specific and unequivocal. The processing must be provided through a positive action from the applicant; this means that tacit consent will not considered as valid, as it has been up until now.
Furthermore, for sensitive data, for instance ethnic origin and health degree, it is required an explicit consent, and this must be ascertainable.

The Accountability principle imposes (to the controller and the processor of the processing) the requirement of being able to prove the compliance of the regulatory predictions with regards to personal data protection.

The GDTR includes another important contribution, the figure of the Data Protection Offices, who will be mandatorily designated by the controller and the processor of the data processing as long as:

II. the processing is performed by a public authority or institution, except of the courts which act in exercise of their judicial functions

III. the main activities of either the controller or the processor consist of processing operations that, by reason of their nature, range and/or purposes, require habitual and systematic observation by the applicants on a large scale. We are referring to here to the private sector.

IV. the main activities of either the controller or the processor consist of the processing, on a large scale, of special categories of personal data, and of data relative to sentences and infractions/offenses referred to in article 10 of GDPR.

The Data Protection Officer will be designated considering his/her professional qualities, aptitudes and Law knowledge. His/her functions will comprise information and advice, compliance supervision, cooperation and contact with the Control/Inspection Authority.
The DPO must act with absolute independence and under the obligation of secrecy and confidentiality.
Another important innovation is the new cooperation and coherence mechanism in the initiation of legal proceedings and in the resolution of penalty proceedings, referred to as "one stop shop" system: it distinguishes between the main control authority and applicant control authority.

The first one is the control authority of the main (or only) establishment of the controller or processor of the processing process, and he/she will be competent to act as control authority for the cross-border processing executed by the

aforementioned controller or processor. The applicant control authority is the authority to whom the processing of personal data affects.

The main control authority will adopt and notify decisions respective to the followed procedures against the controllers or processors, and will inform of those decisions to the applicant control authority and to the European Council of Data Protection. The control authority in front of whom a claim has been filed, will inform the decision to the claimant.

The Spanish Constitution stipulates in its article 18.4: "The Law shall limit the use of data processing in order to guarantee the honor and personal and family privacy of citizens and the full exercise of their rights".
This article was developed by the Organic Law 15/1999, 13th December, on the Protection of Personal Data, valid until the entry into force of the General Data Protection Regulation.

In the Spanish scene, two judgments pronounced by the Constitutional Court stand out after the entry into force of the Personal Data Protection Act (in Spanish, LOPD 15/99).

The first one is the Court Sentence 94/1998, where it is established that the fundamental right to data protection guarantees to the applicant control over his/her data, their use and their destination, so as to avoid their same illicit or detrimental-to-dignity trade. This gets configured as a faculty of the citizen to oppose certain personal data being used for purposes different to those for which its obtaining was justified.

The second one is the Constitutional Court Sentence 292/2000, of 30th November. Here, they distinguished between two different rights: the right to privacy , which allows for certain personal data to be excluded from external knowledge, and the right to data protection, which guarantees the right of availability of these same data to the applicant.

The adaptation of our legislation to the GDTR has involved the necessary devising of a new Organic Law, therefore the legislator has assembled the Organic Law 15/99 about protection of Personal Data.

The fundamental right to personal data protection:

In the Spanish legal order, the right to data protection is set forth in article 18 of the Spanish Constitution. However, it was the Constitutional Court who had to define the principles and rights which would comprise the special content of the same.
The article 4.1 of GDPR stipulates what a personal datum is: "any numeric, alphabetic, graphic, photographic, acoustic information or of any other kind concerning natural, identified or identifiable persons".

According to legal precedents, personal data are:name, surnames and address; ID number; data included in the application for residence; phone number, if it is associated with a person; self image; data of a working register relative to the specific worker; e-mail addresses; and IP addresses.

The Organic Law 15/99 about Personal Data Protection also determines the procedure to be followed in the cases of data protection of deceased people, and deceased people with disabilities.

The fundamental right to data protection rests on two pillars recognized as such by the Constitutional Court: personal consent and the applicant's rights.

In the GDPR a great importance is given to consent regulation, concept which is set forth in the article 4.11 of the same. This article supposes a whole manifestation of free, specific, informed and unequivocal will by means of which the applicant accepts, either via statement or a clear positive action, the processing of personal data which is concerted.

The innovation this regulation includes abides in that the two ways of expressing consent are specified, which may be by means of statement, and by means of an action. Silence, already marked squares or inaction must not constitute consent, which will only be given via positive action and only for specific purposes.

Article 6 of the GDPR stipulates that "data processing shall only be licit if at least one of these conditions is met:

a) the applicant gave his/her consent for their personal data processing for one or several specific purposes;
b) the processing is necessary for the performance of a contract in which the applicant is part, or in order to take steps, upon request of the data subject, prior to entering into the contract;
c) the processing is necessary for compliance with a legal obligation to which the controller is subject;
d) the processing is necessary to protect vital interests of the applicant or of another natural person;
e) the processing is necessary for the compliance of a mission acted in the public concern, or in the exercise of public powers conferred to the controller of the processing;
f) the processing is necessary for the satisfaction of legitimate interests pursued by the processing controller or by a third party, as long as over these interests, the interests or fundamental rights and freedoms of the applicant which require data protection do not take precedent, particularly when the applicant is a child."

In the article 7.3 of the Regulation, the option of consent withdrawal or revocation is considered at any time.

The European legislator has decided to give a specific protection to the use of technology by underage children, and also by adults when they deal with children.
In the article 8 of GDPR the relevant conditions for child consent in relation with the services of the information society are found.

Two premises become enshrined: firstly, the establishment by law of a minimum age of thirteen years, below which the member States will not be able to consider consent as licit; secondly, if the child is under sixteen, consent will only be licit if this was given or authorized by the holder of parental authority or guardianship over the child, being this essential at all events without exception.

The GDPR also assigns the controller the task of verifying if the consent was given or authorized by the holder of parental authority. This Regulation has also regarded special personal data categories, from where the processing of personal data which reveal the following has been prohibited: Ethnic or racial origin; Political opinions; Religious or philosophical convictions; Union affiliation
It is prohibited as well the processing of: Genetic data; Biomedical data aimed at univocal identification of a natural person; Data related to health state; Data related to sexual life or orientation(s) of a natural person.

From this list of special personal data categories, two of them are legally regulated for the first time: genetic data and biomedical data aimed at univocal identification of a natural person.

Despite the fact that these special categories may be processed with explicit consent, it is expected that Union or member States Law will be able to prevent the applicant from inducing this consent, fact which is another innovation.

The GDPR has issued the legal figure of the Data Protection Officer in Spain. With the creation of this new concept, a promotion of the data protection fundamental right is expected.

The Data Protection Officer (DPO) is the responsible person - within the sphere of the processing controller or processor - of the independent supervision and monitoring of the internal implementation and respect for the guidelines of data protection. This DPO may be either an internal employee or an external counsel, *id est*, he/she may take part in the processing controller or processor workforce, or else fulfill his/her functions in the frame of a service contract.

The knowledge and skills of the DPOs must have been acquired through an officially approved formation, since their position is of great relevance, safeguarding and ensuring a fundamental right.
These knowledge and skills are considered essential so as to being able to identify the risks associated to the processing operations, bearing in mind the nature, scope, context and aims of the processing.

In order to guarantee the DPOs working efficacy, their independence in the discharge of their functions has been recognized. Hence, they may neither be dismissed nor penalized by the controller or the processor for the activities they carry out.

The functions of the DPO are stated in the article 39 of the Regulation:

- Information and advice: inform and advise the processing controller or processor and the employees devoted to the treatment of obligations which apply to them;
- Supervision of compliance, responsibilities allocation, awareness-raising and training of the personnel;
- Counsel about impact assessment on data protection;
- Cooperation with the control authority;
- Act as control authority contact point for questions relative to data processing, including the prior consultation.

Distinction among other similar figures to the DPO:

The Compliance Officer:

This figure is developed by virtue of the Directive 2004/39/EC, of the European Parliament and of the Council, of 21st April 2004, on Markets and Financial Instruments.

It define him/herself as the agent appointed by the company who, constituent or not of the organization itself and, with autonomous initiative and control powers, executes an assistance role to the administrative and directive body of the corporation or public and private administrations in compliance with the current legislation, counseling in the identification and institution of controls as well as monitoring the efficacy of the same.
His/her main function consists of the prevention of the offences referred to in the article 31 bis of the Spanish Penal Code, the detection and reaction against the same.

The Controller of the (data) Processing:

The natural or legal person of public or private nature, or administrative body which, alone or jointly with others, decides the purpose, content and use of the processing, even though he/she does not physically execute those.

There may also be controllers of the processing those entities without legal personality acting as separate parties in data traffic; thus, in accordance with the Sentence of the Court of Justice of the European Union (CJEU) of 13th May 2014, on the issue of Google Spain, the search engines may be responsible for personal data processing.

Article 24 of the GDPR sets the controller fundamental obligations, and points he/she is obliged to adopt the technical and organizational appropriate

measures to ensure and be able to prove that the processing is carried out as reported by this Regulation.

The Processor of the (data) Processing:

Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

It is an institution which allows the grant to access the data of those service providers who so require, inasmuch as the processing is carried out on behalf of the controller.

A pretense is considered to have been created by means of which it is understood that data are not revealed to a third party, but they remain under the control area of the controller him/herself, despite the fact that they are managed by a third entity.

The defining element of the controller resides in his/her decision-making capacity so as to determine the purposes and means of the processing while the processor is characterized by finding him/herself subdued to the controller's decisions. It is based on a delegation of tasks in an external organization, legally distinctive, which will process the data in the name of and at the expense of all those who require these services.

RESPONSIBILITIES: criminal, administrative and civil.

The controllers of personal data processing are attributed a series of duties which must be fulfilled in the development of the personal data processing.
The responsibilities in which they may incur during the execution of their actions are framed in the criminal, civil and administrative spheres.

The first sphere involves criminal offences; the second one, the need of

compensation for caused damages; and the third one, deals with infractions and offences committed in the administrative field.

Every data subject will have the right to effective judicial protection when he/she considers that his/her rights, under the Regulation, have been violated as a consequence of a personal data processing process.

Criminal responsibility is found in the article 197 of the Spanish Penal Code. This article establishes imprisonment from one to four years, and fines from twelve to twenty-four months for those who discover the secrets or infringe the privacy of the applicant without their consent.

The same penalties are established for those who seize, use or modify, to the detriment of a third party, reserved personal or familiar data which are registered in files or IT, electronic or telematic support or format, or in any other kind of archive or register, be it public or private.

In order to incur in this kind of responsibility, malice or willful misconduct is necessary. The same applies to another type of actions which may be committed by reckless behavior, such as accessing by mistake or without warning to the files and supports which contain third parties information. From the context in which they are given, it becomes necessary to check that such access has occurred with the purpose of taking profit of that information in order to cause damage to the data owner or to a third party, or to say the least, benefitting from that information.

This way, accidental access to information either by mistake or, due to an inaccurate measure taking by the processing controller, will not result in criminal responsibility.

Article 197 increases the punishment up until five years of imprisonment if the discovered data or facts, or images, are spread, revealed or relinquished to a third party.

Article 197 bis extends criminal protection against those who, along any means or procedure, violating the security measures, and lacking authorization, facilitate to others the access to the whole or a part of the information system, imposing a punishment from six months to two years of imprisonment.

In this new Organic Law on Personal Data Protection, the penalty regime is set in the articles 70 et seq., and distinguishing among minor infractions, serious offences and very serious offences.

The prescription of offences and infractions will be interrupted with cause of the sanctions proceedings initiation with prior knowledge of the interested party, if the sanctioning file was frozen for more than six months by causes non-attributable to the alleged offender.

The Organic Law stipulates the applicable regime to certain specific categories of the data processing controller and processor, among which there are:

a) Constitutional bodies or those bodies with constitutional relevance, and analogous institutions of the Autonomous Communities;

b) Judicial Courts or bodies;

c) The General Administration of the State, the Administrations of the Autonomous Communities and the entities which integrate the Local Administration;

d) Public organisms and Public-Law bodies linked or dependent on the public Administrations;

e) Independent administrative authorities;

f) The Bank of Spain;

g) Public Law corporations, when the aims of the data processing are interrelated with the exercise of public Law powers;

h) Public-sector foundations;

i) Public Universities;

j) The Consortia.

Whenever the afore-cited controllers or processors committed any of the offences referred to in articles 73 to 75 of the Organic Law on Personal Data Protection, the competent data protection Authority will issue a decision sanctioning them under subpoena.

The data protection Authority may decide as well the initiation of disciplinary proceedings. Decisions which fall within those requiring the previous measures and actions, will have to be communicated to this Authority.

The general or main duty of either the data processing controller or processor has been set as that of financially compensating whatsoever damages a person can suffer as a consequence of a processing made in infringement of the GDPR.

There exist two spheres of responsibility: the first one deriving from the breach of the Regulation, fact that automatically calls for the duty of damage compensation; the second one, consisting of the possibility of proving the absence of responsibility in the event or fact that has caused the damage.

The burden of the evidence in this second sphere lies with the controller, who will have to prove that his/her conduct has been assiduous. The party who claims for the damage does not need to prove blame or negligence of the damage originator.

In the cases where the processing controller is a Public Administration, the responsibility will be objective, since this is stipulated as such in article 106.2 of the Spanish Constitution. Even though the conduct meets the Regulation, this does not prevent the duty of financially compensating from enduring, for it is sufficient with proving that the damage has been caused by a misfeasance in the functioning or action of the Administration in order for them to compensate for the damages. It will not be necessary to prove the existence of malice or *mens rea* in the action that caused the damage.

The patrimonial liability regime of Public Administrations is set in Chapter IV, Preliminary Title of the Spanish Law 40/2015 on the Legal Regime of the Public Sector, articles 32 et seq.
In order to appreciate an instance of administrative patrimonial liability, the requirements fixed both in legal and jurisdictional ways must be met.

çIII. Bibliografía:

ADSUARA VARELA, Borja.; <<El consentimiento>> en María Álvarez Caro y Miguel Recio Gayo (coord.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*, Editorial Reus, Madrid, 2016, pp.151-185, p. 154.

ALARCÓN GARRIDO, Antonio. Manual teórico-práctico del Compliance Officer, Sepin, Madrid, 2016; pág. 37.

ÁVAREZ HERNANDO, Javier, <<El Reglamento Europeo y la futura Ley General de Protección de Datos: sus principales novedades>>, Dossier: Manual de las principales novedades del REPD, 2018. pp 7-12, p 7.

Belén Linares, María, Universidad de Sevilla; <<Programas penales de cumplimiento en el seno de la persona jurídica tras la LO 1/2015<<; La Ley Penal nº 118 enero-febrero 2016; Ed. Wolters Kluwer.

El Gobierno aprueba el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal. Diario La Ley. Editorial Wolters Kluwer. 10/11/2017.

FERNÁNDEZ CONTE, Julen y LEÓN BURGOS, Diego., <<Antecedentes y proceso de reforma sobre protección de datos en la Unión Europea>>, en María Álvarez Caro y Miguel Recio Gayo (coord.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*, Editorial Reus, Madrid, 2016, pp. 35-50, en p.37

GARRIGA DOMÍNGUEZ, Ana., <<Nuevos retos para la Protección de Datos Personales: En la Era del Big Data y de la computación ubicua>>, Dykinson, Madrid, 2015, p. 92.

LÓPEZ ÁLVAREZ, Luis Felipe. *Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo,* Francis Lefebvre, Madrid, 2016, p. 26.

LÓPEZ ÁLVAREZ, Luis Felipe, <<La responsabilidad del responsable>>, en María Álvarez Caro y Miguel Recio Caro (coord.), Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad, Editorial Reus, Madrid, 2016, pp. 275-293, p. 277.

NÚÑEZ GARCÍA, José Leandro, <<El encargado de tratamiento>>, en María Álvarez Caro y Miguel Recio Caro (coord.), Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad, Editorial Reus, Madrid, 2016, pp. 321-333, p. 322.

PIÑAR MAÑAS, José Luis.; <<Introducción. Hacia un nuevo modelo europeo de protección de datos>> en María Álvarez Caro y Miguel Recio Gayo (coord.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*, Editorial Reus, Madrid, 2016, pp.15-22, p.19.

PIÑAR MAÑAS, José Luis, <<Novedades en relación con la figura del encargado del tratamiento>>. Publicado en ZABÍA DE LA MALTA, Juan (Coord.) Protección de Datos: Comentarios al Reglamento, Ed. Lex. Nova, Valladolid, 2008, p. 219.

REBOLLO DELGADO, Lucrecio y SERRANO PEREZ, María Mercedes. *Manual de protección de datos*. Dykinson.2014. *Op.cit.pag*. 36

RECIO GAYO, Miguel, <<El delegado de protección de datos>>, en en María Álvarez Caro y Miguel Recio Gayo (coord.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*, Editorial Reus, Madrid, 2016, pp. 367-388, en p. 368.

SERRANO CHAMORRO, Mª Eugenia, <<Protección de datos personales: información, consentimiento y transparencia. Nuevas exigencias jurídicas comunitarias>>. Actualidad Civil nº 5, 1 de mayo. De 2017, Editorial Wolters Kluwer p.6